USA

Latest Updates

- Updated information regarding the PCCP for AI ML and broader medical devices
- Added information regarding AI executive Order
- Updated references to draft guidance that are now final (SaMD, Cybersecurity)

Software	
Embedded Software	Embedded software takes on the classification of the complete device based on its intended use. For devices that have embedded software, FDA has guidance documents that govern the expectations on how the software is developed, validated, and maintained. FDA Guidance - Guidance for the Content of Premarket Submissions for Device Software Functions https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-device-software-functions
Software as Medical Device (SaMD)	Currently, SaMD in US is classified according to its intended use akin to any traditional medical device. Moving forward, FDA is piloting a new model which will classify the software according to the risk-based classification framework published by IMDRF. This framework establishes regulatory qualification and classifications based on the significance of information provided by the SaMD, and the state of healthcare condition treated by the SaMD. FDA Guidance: Clinical Decision Support Software (https://www.fda.gov/media/109618/download) Digital Health Software Precertification (Pre-Cert) Program v1.0 working model (https://www.fda.gov/medical-devices/digital-health/digital-health-software-precertification-pre-cert-program) Note: The precent pilot is on pause since it requires legislative updates to fully support. This will likely be replaced by a Voluntary Approval Pathway with legislative support from Congress. ANSI/AAMI 2700-2-1, is part of a list of standards meant to track the safe use of medical device software in integrated clinical environments (ICE), according to ANSI. The standard is more specifically used to ensure data loggers used in ICE systems are properly able to collect information that can be used to improve and update the system. Issued on 07Nov23.

	ISO IEC IEEE 29119-1: This document specifies general concepts in software testing and presents key concepts for the ISO/IEC/IEEE 29119 series. Issued on 07Nov23.
Clinical Decision Support Software (CDS)	FDA Guidance: Clinical Decision Support Software (https://www.fda.gov/media/109618/download)
Change Management Requirements for Software/SaMD	Current regulations for FDA on software changes to a medical device, including SaMD, determine the need for a new regulatory submission based on the risk of the modification and its impact on core intended use. FDA Guidance: Deciding When to Submit a 510(k) for a Software Change to an Existing Device (https://www.fda.gov/media/99785/download)
Quality Management System (QMS)	FDA has adopted the recommendations from IMDRF regarding the Quality Management System Requirements for Software as a Medical Device. http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-151002-samd-qms.pdf
Post-Market Management	FDA does not distinguish between SaMD and traditional medical devices in terms of their post market requirements. All SaMD products are expected to follow the same requirements from a post market standpoint as traditional medical devices. This includes: Establishment Registration and Device Listing: SaMD manufacturers shall register their establishment and list the devices that are "manufactured" at each establishment - Identifying the device class, and regulated activities performed at each establishment (spec development, Design, manufacturing, packaging, etc). Complaint Handling: Manufacturers are required to gather feedback about the SaMD from service records, service events and complaints. All feedback that meets the definition of a complaint must be evaluated and investigated to ensure continued safe and effective operation of the device. Any complaint that relates to an adverse event must be reported to FDA. See Adverse Event Reporting below. Adverse Event Reporting: Any adverse events must be reported to FDA per 21 CFR Part 803. Product Field Action / Recall: Any action in response to complaint handling, adverse event reporting, or otherwise that is undertaken to reduce a risk to health or correct a violation of the FDA rules and regulations must be reported to FDA as a recall per 21 CFR part 806. Per the precertification pilot program, there are also elements of Real-World Performance Analytics. See V16

Real World Data/Evidence

The FDA precertification pilot program includes an element of Real-world performance analytics where SaMD manufacturers analyze real world data and monitor the performance of the SaMD in the real-world. The specifics of the data collected, and analysis techniques were evaluated within the pilot program. The pilot is now closed, with legislative updates needed to transition to a proposed Voluntary Approval Pathway https://www.fda.gov/science-research/science-and-research-special-topics/real-world-evidence

Artificial Intelligence (SiMD & SaMD)	
Machine Learning	FDA has published a draft guidance on Predetermined Change Control Plans for AI/ML enabled device software functions. It is expected that this guidance will be expanded (or another published) to broadly apply to all medical devices, not just AIML. The law is not limited to AIML. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/marketing-submission-recommendations-predetermined-change-control-plan-artificial
Deep Learning	FDA has published a draft guidance on Predetermined Change Control Plans for AI/ML enabled device software functions. It is expected that this guidance will be expanded (or another published) to broadly apply to all medical devices, not just AIML. The law is not limited to AIML. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/marketing-submission-recommendations-predetermined-change-control-plan-artificial
Best Ethical Practices	No updates at present.
Generative AI	US President has issued an executive order for the safe, secure and trustworthy AI. The Executive Order establishes new standards for AI safety and security, protects Americans' privacy, advances equity and civil rights, stands up for consumers and workers, promotes innovation and competition, advances American leadership around the world, and more. Each government agency has 180 to 270 days to develop their own regulations and guidance pursuant to the executive order.

Cybersecurity
FDA final guidance on premarket management of Security: Final Guidance: Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions. Issued September 2023 Final Guidance: Post market management of cybersecurity in medical devices. issued December 2016 Cybersecurity for networked medical devices containing off-the-shelf software. issued January 2005

ANSI AAMI SW96:2023: Provides requirements on methods to perform security risk management for a medical device in the context of the safety risk management process required by ISO 14971. This document is intended to be used in conjunction with AAMI TIR57 and AAMI TIR97. Issued on 07Nov23.

Data Privacy

FDA does not regulate Privacy as their congressional mandate is limited to Public Health. Data protection regulations and data privacy laws are enforced by the U.S. Federal Trade Commission (FTC). Most regulation however are at the state level.

All 50 states have adopted some form of breach notification laws, data disposal laws and data privacy laws, although there may be differences in the definition of personal data and in what constitutes a data breach. The most well-known among these is the California Consumer Privacy Act (CCPA), which has spawned similar regulations in at least 9 other states.

From a healthcare / medical device perspective, there is Health and Human services enforces the Health Insurance Portability and Accountability Act (HIPAA) which regulate how individual protected health information is shared between healthcare providers and establishes penalties for non-compliance.

Labelling

UDI	US FDA has an established UDI Rule since 2014 - all devices are required to have a UDI on the label, with corresponding data submitted to the Global Unique Device Identifier Database (GUDID)
Specific Market Requirement	SBOM, Cybersecurity Patch Management Plan